AU/AFFP/HARVARD/2002

AIR FORCE FELLOWS PROGRAM

AIR UNIVERSITY

# ARES, JANUS, GLOBALIZATION

# A PRIMER FOR THE MILITARY LEADER IN NATO

by

Dean R. Clemons, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr Anthony G. Oettinger
Harvard University

Maxwell Air Force Base, Alabama

April 2002

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **00 APR 2002** | **N/A** | **-** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Ares, Janus, Globalization A Primer For The Military Leader In Nato** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Maxwell Air Force Base, Alabama** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **UU** | **68** | |

## Disclaimer

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the United States Air Force, the Department of Defense, or any other government agency or department.

## *Abstract*

War and human life have been coupled since before antiquity. Ares, the Greek god of war, wielding fist and sword, battled with immortals and mortals alike. In more recent times, as economies and politics become increasingly interdependent—or, globalized—Janus, the Roman deity of doorways and passageways, who watched in two directions at once, has begun to take center stage, looking at both international stability and security.

This study examines globalization from the perspectives of three interlocking stakes: international military and commercial investment; dual-use technologies; and export control. As a primer on these stakes for the rising military leader within the North Atlantic Treaty, the study elucidates the issue of cooperation vs. competition intrinsic to NATO and the European Union as together they seek to increase transatlantic security. The enormous potential of dual-use technologies is examined, with a focus on the *angst* of military leaders about the increasing dependence on technologies that are widely commercially available to both friend and foe. Last, the competing demands of openness of markets and of international security involved in both those stakes lead to consideration of the economic instrument of export control of technologies.

Globalization is irreversible. To be successful in future conflicts, the rising military leader will need to be fluent not solely in military affairs but also in the languages of economics and politics. Like globalization, coalition warfare is here to stay, and although, for that reason, interoperability of both systems and organizations remains desirable, competing demands of national economies pose significant challenges to achieving it. To meet such competing economic demands, the military leader of tomorrow will need to

employ dual-use and science and technology programs to the advantage of the U.S. military and the NATO alliance. By clearly articulating warfighting requirements and shortfalls and by understanding existing programs and processes, the military leader will be able to influence the export control process. Conflicts will undoubtedly occur in the twenty-first century, and the rising military leader will need to learn to leverage investment, dual-use technology, and export control laws to mitigate actual bloodshed.

## *Acknowledgements*

This study is the result of the work and play of a team of people. Its faults are entirely mine, because, without doubt, the others on the team provided flawless assistance from their own domains. I thank them for their patience, kindness, and generosity, which were equalled only by their expertise.

I first thank Professor Anthony G. Oettinger, chairman of the Program on Information Resources Policy at Harvard University, who mentored me throughout the research on and writing of this paper. I thank him for sowing some seeds that taught me to ask good questions in peace as preparation for just, swift, and accurate decisionmaking in war. I thank John C. B. LeGates, for his tremendous logistic support and his quiet introductions of me to learned men and women, many of whom influenced this paper and all of which changed my horizon. I thank Dr. Ellin Sarot, for awe-inspiring expertise as an editor and an uncanny ability to find wheat, discard chaff, and bake bread all the while the farmer kibbitzed beside the desk. I thank Margaret S. MacDonald, for sharing remarkable and unique insights into European political and economic dynamics. More important, I thank her for sharing her generous intellect and spirit. Without them, this study could not have been written. I thank Claire Merola Bishop, Mary C. Walsh, and Maria L. Waite for their tireless support and encouragement. I thank Rohan Kariyawasm for providing a sounding board on issues of globalization and law. On many occasions,

his grasp of decisionmaking within the European Union and his provocative strategies to mitigate violence in South Asia focussed my thinking.

On a personal note, I thank Kerry Murphy for her incredible courage and for her support of the Clemons family in a difficult time. Finally, I thank my wife, Lisette, for lovingly writing another chapter in our lives, and my sons, Isaac and Aaron, who will continue to teach me how to love, on earth and in heaven.

## *Contents*

*Page*

## *Illustrations*



## *Tables*

*Page*

## Chapter One

# Introduction

> *Globalization and the information revolution bring enormous benefits to the transatlantic community, including its security structures, but they also increase its vulnerabilities.*[1]
>
> William S. Cohen,
> Former Secretary of Defense

Since the terrorist attacks on the World Trade Center in New York City and the Pentagon on September 11, 2001, people "on the street" have repeatedly said that nothing will ever be the same, that terrorism of this magnitude in the United States is new and different. In the words of President George Bush, "And night fell on a different world."[2] In an immediate sense, yes. Within weeks, the United States and its transatlantic allies were involved in a military effort in Afghanistan to root out El Qaeda and, in particular, to locate Osama bin Laden. Yet, in a broad context, issues of national security, international commerce, and international cooperation have retained their previous primacy and fundamentally remain unchanged. In a globalize world, these issues, however difficult, complex, and even thorny, are also crucial to international stability and security.

War has occurred before and within recorded history. Historians of antiquity wrote about it in detail. In the myths of the Greeks, Ares, Zeus's son by Hera, was the god of war. A wild, ungovernable deity, Ares slashed about the countryside accompanied by his

sons, Phobos (Panic) and Deimos (Fear). They loved battle for its own sake, loved it with no regard for the suffering it brought. In the present, if the late twentieth-century is an indicator, the twenty-first century will be marked by an impressive move toward globalization, that is, an interdependence of economies accompanied by the striking of strategic alliances on a scale perhaps never before seen in history. What is certain is that globalization is irreversible. Ares and sons may roam the global country-side, but today their aggressiveness will be met and tempered by the force of modern-day realities, often realities with opposing faces.

The rising military leader in today's (2002) North Atlantic Treaty Organization (NATO) will need to understand the globalize environment and its nuances. Civilian leaders in the United States and in other countries will need to be able to count on the informed counsel of the military leadership as together they strive to defend both nations and alliances. A military leader will need to recognize that in a dynamic, multipolar, post-cold war environment, rogue states, transnational migration, and terrorism have posed and will continue to pose real threats for years to come. A military leader will need to be aware of all the instruments of national and international power—as successful military officers in the past, such as Washington, Eisenhower, and Marshall,[3] were.

This study offers a primer on three stakes and their stakeholders in a globalized world, a primer that the military leader in the twenty-first century may be able to apply immediately as well as use as a springboard for further study. Because globalization, like the blind men's elephant, feels different depending on one's point of contact, the focus of this study is on international military and commercial investment, dual-use technologies,

and export control and administration. The scope is limited to transatlantic security, and from this perspective the reader is invited to extrapolate broader, more global lessons.

Fifty-two years after it was established, NATO still undergirds world security. Since its inception, member nations have agreed that

> an armed attack against one or more of them in Europe or North America shall be considered an attack against all of them…and each of them will assist the Party or Parties so attacked.[4]

As evidence of NATO's strength, Central and Eastern European nations clamor to be recognized as "partners for peace" or as full members.[5] Zbigniew Brzezinski postulated that a larger, more secure Europe will clearly be a central issue confronting world leaders in the twenty-first century.[6]

The critical links between global commerce and international security have been recognized for some time—since, for example, the Marshall Plan (1947–52) or the Maastricht Treaty (1991), establishing the European Union—but what is new is the "cyber era" and in this era the increasing risk and challenge of information technology that is used by both business and military planners.[7] What should not be news is that both the deliberate use of export control protocols and the judicious use of dual-use technologies are fundamental to transatlantic security.[8] Nor should it be news that corporations, national and international, want to achieve an advantage over their competition, or that a national economic advantage often gives way to international security concerns. Such competition exists even though Article II of the North Atlantic Treaty calls on member nations "to eliminate conflict in their international economic policies and…encourage economic collaboration between any or all of them."[9]

Also not news is that interoperability—of systems and organizational structures—remains an elusive objective within U.S. forces and among the NATO allies.[10] Military officers and many of their civilian counterparts already recognize that without interoperability effectiveness in war is reduced.[11] Yet the criticality and urgency of interoperability have not led to implementation.

### 1.1 Objective and Scope

The objective of this study is to examine the elephant of complex "globalization" from the touching points, or perspectives, of three primary interlocking stakes: international military and commercial investment; dual-use technologies; and export control. Issues in the globalization of national security, international commerce, and international cooperation, like Janus, another ancient deity—the Roman god of passageways and gates whose two faces look in different directions at once—have more than one face. The stakes for international security and prosperity within globalization are extraordinarily complex and high, and there is no "silver bullet"—no one neat and easy solution for all the questions and issues involved.

The main stake examined is transatlantic security as it was established and is practiced by members of NATO. As a primer for the military leader within NATO, this study accepts the premise that the military leader is the primary stakeholder. Insights into that premise will be useful also to the congressional stakeholder in the United States, the parliamentary stakeholder in the United Kingdom (U.K.), and the global commercial-sector stakeholder. For balance, issues are included that are pertinent to the Russian Federation, China, and even "rogue states," with respect to their relationship to NATO's defense and economic structures.

## 1.2 Structure

The study consists of five chapters, three of which present separate perspectives on globalization, although each perspective is, of course, related to neighboring ones and together they constitute the big picture. **Chapter One**, this introduction, provides a background through discussion of transatlantic security, the North Atlantic Treaty, globalization of economies, and the intrinsic cooperation and competition of global economic partners.

**Chapter Two**, the first of the three perspectives on globalization, opens with an examination of the relationship of NATO to the European Union (EU), given that both organizations are cornerstones of international security. The chapter proceeds to the need for interoperability of systems and organizations to support coalition warfare, the type of warfare most likely to occur in the twenty-first century. It next looks at the inherent competitiveness of international markets, an attitude potentially opposed to achieving interoperability, and then examines international defense spending and investment, with a focus on defense spending as a percentage of the gross domestic product (GDP). The chapter concludes with a discussion of the necessary reliance by all member states on the commercial sector to retain NATO's superiority in defense.

**Chapter Three** concentrates on dual-use technology and diffusion of technology in relation to globalization. A definition of dual-use technology is offered with the suggestion that, given NATO's growing reliance on commercial industry to retain security dominance, the expansion of dual-use is probable. The chapter examines the possible *angst* at the heart of this issue caused by the prospect of over-reliance on technologies that may be in the hands not only of allies but also of adversaries and by the potential for both legal and illegal global diffusion. The Internet is used here as a model

to highlight difficulties in controlling technology which adversaries of NATO might use in their own military applications.

**Chapter Four** examines the history of the use of export control and the waning applicability of export control in a globalized world. The relationship between dual-use technologies and export control is discussed, particularly the importance of focussed controls as well as some points of failure in current (2002) export control. The intention here is to shed light on U.S. congressional and U.K. parliamentary debates on export control. International efforts to control technology also are discussed, with an emphasis on the need to bolster current programs without creating a deadlock for legitimate enterprise.

**Chapter Five**, which presents conclusions and suggestions, consolidates the three perspectives delineated in the previous three chapters and draws rudimentary conclusions as to the actual the look and feel of globalization. The suggestions are meant to be open-ended, consistent with the method of the Program on Information Resources Policy, which is to say, not prescriptive by design. They are intended, rather, to provoke additional thought and discussion in the ongoing dialogue about the globalization of economies and the accompanying security issues.

## Notes

[1]William S. Cohen, "Preface," *Strengthening Transatlantic Security, A U.S. Strategy for the 21st Century* (December 2000). Cohen was Secretary of Defense in during the Clinton administration (in 1997-2001).

[2]President George Bush, Address to a Joint Session of Congress and the American People, on 20 Sept. 2001, [On-line]. URL: http://www.whitehouse.gov/news/2001/09/20010920-8.html (Accessed on 21 Feb. 2002.)

[3]And unlike, for example, Ulysses S. Grant.

[4]Article V, North Atlantic Treaty, Washington, D.C., 4 April 1949, [On-line]. URL: http://www.nato.int/docu/basictxt/treaty.htm (Accessed on 5 Oct. 2001.) The member nations of NATO are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France,

Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Republic of Korea, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and the United States.

[5]In 1999, the Czech Republic, Hungary, and Poland became members of NATO; other countries supported for membership following the 1999 Washington summit are Albania, Bulgaria, Estonia, Latvia, Lithuania, Macedonia, Romania, Slovakia, and Slovenia.

[6]Zbigniew Brzezinski, "America In the World Today," in *Complexity, Global Politics, and National Security* (Washington, D.C.: National Defense University, Institute for National Strategic Studies [INSS]), 29-31. Brzezinski was an advisor to the Kennedy and Johnson administrations and national security advisor to President Jimmy Carter. See CNN Perspectives Series [On-line]. URL: http://www.cnn.com/SPECIALS/cold.war/kbank/profiles/brzezinski (Accessed on 16 Jan. 2002.)

[7]Peter H. Daly, The Roles of Business and Government in Cyber Era National Security, (1999), [a study plan no longer available from the Program on Information Resources Policy]. See Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=424 (Accessed on 21 Feb. 2002.)

[8]Military export controls have been an element of U.S. security since before world War II; see the Center for Strategic and International Studies (CSIS), Executive Summary, *Computer Exports and National Security: New Tools for a New Century* (Washington, D.C.: CSIS Press, A Panel Report of the CSIS Commission on Technology Security in the Twenty-First Century, June 2001), xiii–xxii, [On-line]. URL: http://www.csis.org/pubs/ (Accessed on 28 Feb. 2002.)

[9]Article II, final sentence, North Atlantic Treaty, [On-line]. URL: http://www.nato.int/docu/basictxt/treaty.htm (Accessed on 5 Oct. 2001.)

[10]Anthony W. Faughn, *Interoperability: Is It Achievable?* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, September 2001), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=555; and William F. Maher, Jr., *Legal Aspects of State and Federal Regulatory Jurisdiction Over the Telephone Industry: A Survey* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-85-3, March 1985), [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?ID=44

[11]See, for example, *Kosovo/Allied Force After-Action Report*, Report to Congress, Dept. of Defense, 31 Jan. 2000, [On-line]. URL: http://www.defenselink.mil/pubs/kaar02072000.pdf (Accessed 12 Feb. 2002.)

# Chapter Two

# Transatlantic Security, Interoperability, and Investment

> *It is logical that the United States should do whatever it is able to do to assist in the return of normal economic health in the world, without which there can be no political stability and no assured peace.*[12]
>
> General George C. Marshall

## 2.1 The North Atlantic Treaty and the EU: Cornerstones of International Security

In April of 1949, the United States and several of its European allies consummated a mutual interest in collective security by signing the North Atlantic Treaty. By staying committed to its articles, the resultant organization of states became one of two cornerstones not just of Atlantic security but also, arguably, of global security. Most military officers and civilian leaders are familiar with Article V of the Treaty, which, as quoted in the previous chapter, provides that an attack against one constitutes an attack against all and allows for a collective military response.

The United States and its NATO allies remain intensely committed to Article V and have shown their resolve to support expansion of the Area of Responsibility (AOR) as recently as 1999, in operation Allied Force, by employing military forces in Kosovo. Fundamentally, the NATO members have a vital interest in preserving peace and stability in Europe, and even in the post-cold war environment NATO will continue to keep forces in Europe. According to William S. Cohen, "the presence of significant and highly

capable U.S. forces in Europe will remain, for the foreseeable future, a critical linchpin."[13] Article V of the North Atlantic Treaty was invoked within a day of the September 11 attacks, providing powerful testimony to NATO's overall approach to collective security.

In the globalized environment, Article II of the North Atlantic Treaty is primary, and in day-to-day interactions it is likely to provide the stability and security that leaders seek. For this reason, the article is worth studying in some detail. In part it states:

> The parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions… and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.

The military establishment will need to recognize that in times of peace the United States and its allies are vital stakeholders in ensuring and furthering Article II, and, should such support fail, the United States and its allies may pay for failure with blood. They will increasingly need to complement their warfighting tools with economic tools that cross oceans to provide security by design, not by happenstance.

Military officers and their civilian leadership need to understand that NATO is one of twin security cornerstones, the other being the European Union. Together these gemini provide the foundation of stability for international security and, for that reason, are best studied in parallel. As one twin thrives so will the other, as one is bloodied so will its twin.

It cannot be a surprise that Europe and the United States are tightly linked in the economic instrument of national security and power. The EU is cousin to the Marshall Plan with a greatly expanded international economic symbiosis. Interestingly, many

people (including this author) have believed, erroneously, that in the aftermath of World War II the United States was wholly charitable in its financial support of both allies and the former Axis partners, but the United States and its economy also benefited from this charity.[14] U.S. aid was economic—that is, until 1953 (during the Korean conflict), it did not include military aid.[15] The merging of economic and military aid with a global reach was an important harbinger of the future, of the EU and NATO.

The EU is the United States's largest trading partner and likely to remain so in the twenty-first century. In 1999, the two-way trade between the United States and Europe was $507 billion. The United States has invested nearly $4.5 trillion in Europe, and Europe has invested a similar amount in the U.S. economy. This two-way trade has accounted for 14 million jobs in a single decade, and the economies of the EU may soon surpass the U.S. economy as the largest in the world.[16]

Key to international security are continuing and stalwart support for collective security along with an increasing recognition of the programs, processes, and organizations that can implement Article II of the North Atlantic Treaty. A byproduct of strengthening the link between NATO and the EU may be improved economic performance with a commensurate increase in resources that could then be used to improve both national defense capabilities for the United States and the member countries of NATO and the EU.[17]

### 2.2 Interoperability: Critical to NATO's Coalition Operations

In war, interoperability is not free, and without it NATO would be less effective than it needs to be and will need to be in the future. Since Goldwater–Nichols in 1986,[18] the U.S. military has been in the process of transformation from a platform-based responding

force into a force that fights in "network-centric" fashion,[19] requiring the United States and its allies to continue to improve "sensor-to-shooter" capabilities. An effective network and network-centric capabilities stress the need for interoperability.

In March–June 1999 in Kosovo, NATO's operation Allied Force[20] reinforced the need for interoperable forces, but it also, according to Admiral William Owens, confirmed a "significant gap" between the military capabilities of the United States and its allies: Owens pointed to precision-guided munitions, satellite reconnaissance communications, and other modern technologies as areas of the disparity. The United States and its allies have not yet got "there."

Some of the technologies in which NATO has shown a lag in interoperability are available through export or diffusion, yet, according to Admiral Owens, in warfare that will involve NATO partners serious problems lie ahead, because "a root premise of coalition warfare is that the partners be able to work together and that their military components…be coordinated seamlessly."[21]

The path to network-centric warfare will need to include interoperability, but inter-operability is complex and the path to it has many forks. A recent (2001) review of coalition operations has shown that the political and economic dimensions of interoperability may be manifested at strategic, operational, tactical, and technological levels,[22] and to fight effectively in the future, as Lieutenant General Joseph Kellogg of the Joint Chiefs of Staff has emphasized, the intent of architectures will need to be "a seamless, end-to-end system of fully networked capabilities."[23]

Given that the United States and its NATO allies all share a vision of interoperable systems, it would seem that interoperability would be achievable. Indeed, the DOD's

policy on inter-operability is broad and sounds inclusive of NATO allies and potential coalition partners:

> Interoperability within and among United States forces and U.S. coalition partners is a key goal that must be addressed satisfactorily for all Defense systems so that the Department of Defense has the ability to conduct joint and combined operations successfully.[24]

The DOD's acquisition policy appears to recognize the link between defense and economic stability:

> In order to foster interoperability with its allies and coalition partners, consideration shall be given to procurement or modification of Allied systems or equipment, or cooperative development opportunities with one or more Allied nations to meet user needs.[25]

Thus, the problem with interoperability policy is not the policy but, as with most policy, implementation and enforcement.[26] Ensuring interoperability with NATO allies runs smack into a huge stake: competition vs. cooperation. Although to this point the background given here has emphasized the cooperative nature of NATO and the EU, the competitive nature of the globalized world also has ramifications for international security.

### 2.3 Economic Cooperation and Competition: Toward Achieving Interoperability

Through fifty-years plus the relationship of the United States and its NATO and EU partners has proved abiding, based as it is on a shared need for stability. Fifteen nations are involved, each and all possessing some degree of nationalist fervor and with individual economies to foster. As each nation assesses the military threat to itself and to its populace, it routinely reassesses its commitment of resources to defense in an effort to balance commitment and other national objectives. No nation has infinite resources or

zero threat to its people. The reassessment of resources by independent nations gives rise to stakes of economic cooperation and competition that put interoperability and "seamless" coalition operations in jeopardy. The situation is complex, as in Kosovo, where both sides of the Atlantic partnership fought as a coalition, not as independent nations. Only a few years later, the multinational military response in Afghanistan to the terrorist attacks on the United States in September of 2001 again indicated that coalition warfare is likely in the twenty-first century.[27] The dependence on coalition warfare brings with it a need for interoperable systems, but support for national defense often may override concern for collective security. The opportunity for cooperation contains the serious hurdles of national economies.

With a two-way trading bloc measured in the trillions and known shared security concerns that burden all fifteen nations, the call for cooperation would seem self-evident. Yet, for instance, the relationship between the EU and the United States has begun to sour over U.S. defense mergers, mainly because beginning in the early 1990s Europe has taken a serious economic hit in its defense-related industries. Owing to international competition, during the 1990s the United States's staunchest allies—Britain, France and Germany—lost at least 100,000 high-paying, high-tech defense jobs, resulting in a lopsided transatlantic defense trade in favor of the United States.[28]

The U.S. military-industrial-complex-centric reader may object to acknowledging this souring relationship, given known shrinkages in the U.S. marketplace. For example, during that same period, the United States experienced widespread consolidation of defense firms driven primarily by a shrinking of the defense budget by 70 percent.[29] The U.S. domestic market has shrunk from a high of 120,000 defense firms in 1990 to a low

of 30,000 defense firms in 2000—yet the surviving firms managed to grab 40 percent of the global market where it had held only 25 percent ten years before. Current (2001) procurement budgets for all EU nations cannot ensure the long-term survival of even one-third of European defense firms, thus the sour taste in European mouths.[30]

Although cooperation among nations appears to be the answer for interoperability, international competitive market forces have been increasing. Free trade would allow acquisition of equipment and systems at reasonable prices and ensure interoperability by excluding noncompetitive manufacturers. As Jacques S. Gansler, under secretary for defense for acquisition, noted in 1998, cooperation in the geopolitical, military, and industrial arenas and removal of inefficiencies could "improve transatlantic industrial ties" and, by default, improve goods and services while recognizing the political realities of providing countries a fair return on their investments.[31]

The United States's allies have economic reasons for not cooperating unilaterally with the United States. As **Table 2-1** shows, the computer industry, for example, is ripe for competition among the NATO allies. Simply put, the allies have their own indigenous manufacturing, assembly, and research capabilities in the computing industry, which directly competes with that of the United States, and their desire to further their own marketshare and economic advantage does not always synchronize with international security concerns. The computer industry is not alone in the globally competitive environment. Military arm sales and "high technology" mirror a similar international competitiveness. As manufacturing becomes global, more and more countries enter the economic fray for their own economic gain, with little thought of aiding or abetting the United States's economic advantage. The United States's silver crown as "king of the

global high-tech market" is rapidly being tarnished by attacks as adversaries and allies alike rush to build their own organic capability.[32] The National Science Foundation (NSF) has estimated that although the United States may retain the largest share of the high-tech market, the dimension of its share has dropped from roughly 25 percent in 1991 to18 percent in 2001 as new economies continue to enter the market.[33]

**Table 2-1. Manufacturing, Assembly, and Research Capabilities of Allied and Adversarial Countries**

| Country | Computers | Components | Software | Research |
|---|---|---|---|---|
| Belgium | | I | I | I |
| France | I | | I | I |
| Germany | I | | I | I |
| Italy | I | | I | I |
| Netherlands | I | | I | I |
| United Kingdom | I | I | I | I |
| China | I | I | I | I |
| Russia | F | I | I | I |

Source: U.S. Department of Commerce; Merrill Lynch; Gartner Group. Data adapted from Table 2.1 in "Computer Exports and National Security" in *New Tools for a New Century* (Washington, D.C.: Center for Strategic and International Studies [CSIS], June 2001), 7.

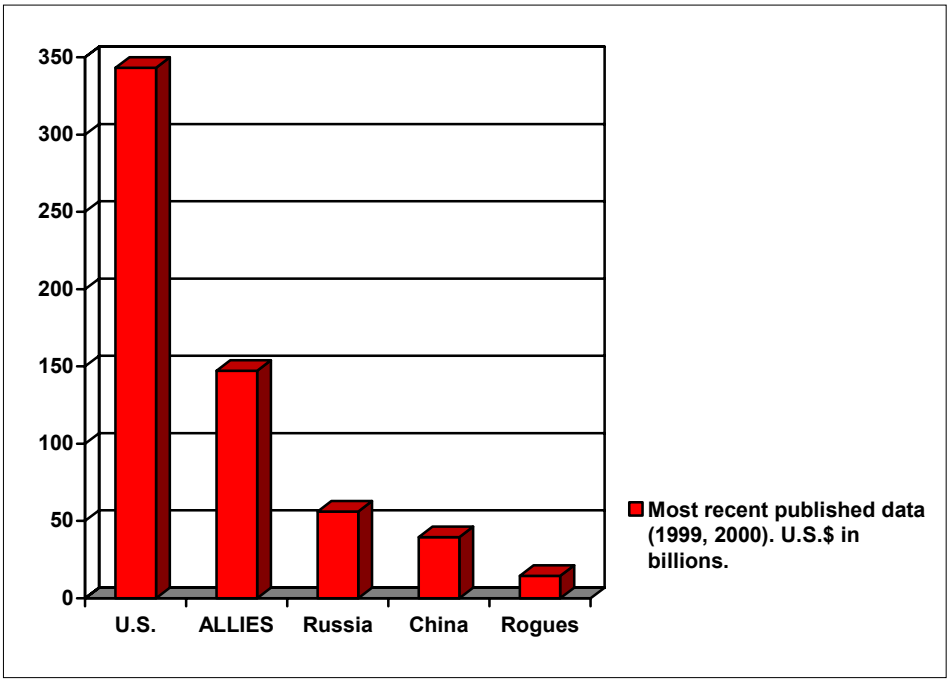
I = indigenous capability F = capability from foreign subsidiary

## 2.4 International Investment in Defense: Driver of Economic Cooperation or Competition

To no one's surprise the United States, the single remaining superpower, with military commitments throughout the globe, spends more on its military than any other nation (see **Figure 2-1**). What is remarkable is not that it spends more but that the disparity between what the United States spends and what its allies in NATO and the EU spend is enormous. For instance, in an alliance that values collective security, the United States spends more than two times what all its allies combined spend. It spends a

whopping $343.2 billion, compared with $147.219 billion for all other nations in the alliance combined.[34] It spends 10 times more than its closest ally, the U.K., which spends only $34.5 billion; only four (France, Germany, Italy, and the U.K.) of the other 18 countries comprising both NATO and the EU spend more than $10 billion. Eight of the NATO and EU member nations spend less than $3 billion—the approximate cost of a single U.S. B-1B bomber. Iceland, which can be said to function as a stationary platform—an aircraft carrier—for the alliance, contributes only $19 million, that is, less than the cost of a single military supercomputer.

One may argue that the United States also spends an inordinate amount compared to its likely adversaries. For instance, it spends 23 times more than the $14.4 billion spent by all "rogue" nations combined, as these are identified by the Pentagon (see Figure 2-1). The United




Note: Allies include all NATO countries excluding the United States and Rogues—the United States's most likely adversaries, in the view of the Pentagon: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

Sources: International Institute for Strategic Studies, U.S. Department of Defense; *The Defense Monitor* **XXX**, 7 (August 2001).

**Figure 2-1. U.S. Military Spending vs. the World**

States spends 6 times more than Russia, which spends $56 billion, and 8 times the military budget of China, which spends $39.5 billion. Indeed, the total military budgets of the United States and all its allies combined are greater than the total military budgets of Russia, China, and the seven rogue nations combined.

Again to no one's surprise, as the sole superpower the United States spends this amount of dollars on defense because its stated defense goal is to "preserve an American technological edge" and its premise in a globalized world is to be able always "to maintain superior status in a technologically stratified international system."[35] Although the dollar amount may seem enormous in relation to what allies of the United States spend, the historical trends of the military percentage of the United States GDP tell a different story, one with potentially catastrophic implications for modernization and for retention of a technological edge.

In 2001 the amount of money the United States spent on defense, as a percentage of the GDP, was at the lowest it has been since 1940. From more than 6 percent of the GDP in 1989 in 2001 it hovered at around 3 percent of the GDP.[36] The power of the United States on the world stage may slip when it is recognized that, although "modernization" is 30 percent of the DOD's budget for fiscal year (FY) 2002 and the DOD's goal is 3 percent of the Total Obligation Authority (TOA), the current (2002) Presidential Budget was only 2.7 percent of the TOA. The Services, too, are struggling. In 2001 funding for Science and Technology, for example, was only 2.1 percent of the Air Force TOA.[37] Several current and former prominent members of the U.S. military have publicly denounced as insufficient the current budget of 2.9 percent of GDP, saying that the U.S. military is heading for a "train wreck" because of its inability to recapitalize the force or

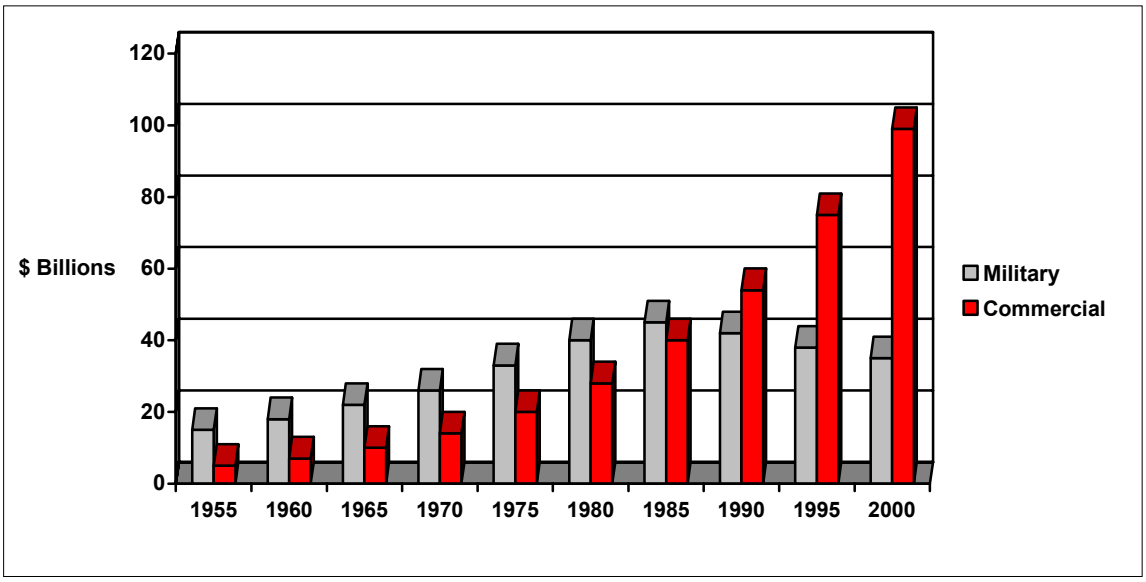
to sustain current readiness on that budget.[38] They have said that the changing world environment, the need to sustain readiness, recapitalize, modernize, and transform the U.S. military mandates that the military budget rise to at least a "four-percent solution."[39]

### 2.5 Growing Reliance on Commercial Technology: Harbinger of the Future?

Compounding the problem of disparate military and commercial spending on research and development (R&D) is the growing awareness that the U.S. military neither leads in innovation nor drives technological advances. It increasingly relies on commercial technologies, many of them available on the open market for consumption by friend or foe. What should alarm the military leadership is that in the globalized marketplace the commercial sectors in the United States and elsewhere pay very little attention to national boundaries. The reliance of the U.S. military on information superiority to enable new operational concepts of dominant maneuver, precision engagement, focussed logistics, full-dimensional protection, and, through their synergy, full-spectrum dominance[40] increasingly depends on a commercial sector that pays scant attention to national boundaries.[41] Unfortunately, the commercial sector, as is widely accepted, leads in advanced technology integrated into modern information-intensive systems. This is especially true in the software and the consumer microelectronics sectors.[42]

The erosion of the DOD's dominance in technological advance is not new, nor is its need to look to the commercial industry for technological advance. **Figure 2-2** tells of the demise of the U.S. military's prominence in technological advancement between 1955 and 2000. Although the DOD's initial investment in 1955 was $15 billion, that sustained only a 4 percent escalation until the mid-1980s and achieved a maximum of $45 billion in

1985–86. After that, the accepted decline in R&D spending has led to only $35 billion for R&D in 2000. At the same time, the commercial industry began in 1955 with only a $5 billion investment in R&D but has sustained an annual growth rate of 7 percent since then and in approximately 1985 crossed over the DOD's spending in this area.




Source: *Naval Research Advisory Committee Report*: *Science and Technology* (June 2000), 15, [On-line]. URL: http://nrac.onr.navy.mil/ (Accessed on 15 Jan. 2002.)

**Figure 2-1. U.S. Military vs. Commercial Spending on R&D**

According to commercial forecasts, industry will continue the 7 percent commitment for the foreseeable future, and the trend toward military reliance on commercial technology will grow.[43] The implication for the military is astonishing: a mandate to incorporate commercial technologies that may or may not be exclusive to the U.S. military or its allies. For this reason, the military leader of the twenty-first century will need to become familiar with cooperative economic strategies for the military and the commercial sectors. A reasonable launch point would be to break down the barriers of "fortress defense" and "fortress industry." It rests with military leaders to issue a positive articulation of the military's technological needs. With respect to the EU partners, the

U.S. military leader will want to recognize that the United States's long-term (five to ten years) technological development needs to be conducted in collaboration with competitors in the EU. For reasons of interoperability, performance, and cost, the DOD will need to take advantage of commercial technology and participate in framing the requirements for industry.[44] According to Gordon Sullivan, of the *Tacoma News Tribune*:

> The good news today is that American military power is still vastly superior to all likely competitors, in most categories, and barring any sudden technological breakthroughs, U.S. supremacy for a decade to come is assured.[45]

**2.6 Investment in Niches to Achieve Technological Advantage in Warfare**

The U.S. military leader of the twenty-first century will need to see that U.S. investment, though limited and shrinking in relation to the previous year's GDP, remains an important weapon of the security arsenal. For the United States and its NATO defense partners to remain dominant in international security, they will need to look at technological niches where the commercial sector does not participate.

Military leaders conversant with the DOD's Science and Technology Program—actually, the rubric for a cluster of subprograms that explore many scientific and technological areas—will apply them to security at home and abroad. The science and technology investment is a critical instrument for U.S. military leaders in order to implement Article II of the North Atlantic Treaty, which empowers the United States to counter military threats, and the article expands policy-makers' options to include those other than war to promote stability and prevent conflict.[46] Military leaders will be needed who can articulate the warfighters' requirements to the science and technology community, to make it sensitive to the opportunities the military niche presents for international security. The DOD's Science and Technology Program was organized to

support the missions described in the National Security Strategy (1995)—missions intended to respond to the strategy's goals and objectives, among them, preservation during a conflict of an information advantage over the adversary.[47]

### 2.7 Summary

The United States and its NATO allies remain committed to the articles of and principles of NATO. In a post-cold war environment, the military leadership on both of sides of the Atlantic have a burgeoning requirement to familiarize themselves with the means to implement Article II of the North Atlantic Treaty, and, should efforts to maintain stability fail, they will need to conduct operations as a coalition. Although recent experience, in Kosovo and in Afghanistan, has proved that doing so requires extensive interoperability of systems and structures, the disparity between the systems of the United States and its allies is growing, which is damaging to the prospects of achieving interoperability.

An examination of the globalized environment and of the allied commitment of resources to military and R&D budgets offers a partial explanation of the phenomenon of noninteroperability. Nation states act in their own interests, and the business of defense and its subsidiaries such as high technology are lucrative for individual nations, which therefore are not always compelled to act to improve the collective security of all NATO partners. The U.S. investment by far outweighs that of even its allies, yet its investment in defense has been shrinking as a percentage of the GDP and its ability to fund advances in technology has begun to wane. This situation has necessitated a growing reliance on commercial technological sectors to implement the U.S. network-centric model of warfighting.

With this environment as a backdrop, proponents of Articles II and V of the North Atlantic Treaty look for cheaper yet dependable alternatives in order to achieve international security. The movement to and employment of dual-use technologies and export control to retain international security has been growing in prominence, but there are many ramifications of this move, both in the stakes and for the stakeholders in these domains. The next two chapters address these stakes in detail and highlight the potentialities and the pitfalls.

## Notes

[12]Excerpt from a commencement address by George C. Marshall, Secretary of State, "On June 5, 1947,…at Harvard University, [when he] first called for American assistance in restoring the economic infrastructure of Europe. Western Europe responded favorably, and the Truman administration proposed legislation. The resulting Economic Cooperation Act of 1948 restored European agricultural and industrial productivity. Credited with preventing famine and political chaos, the plan later earned General Marshall a Nobel Peace Prize. The Economic Cooperation Act of 1948, April 3, 1948, page 1, General Records of the United States Government, National Archives and Records Administration [S.2202, 80th Congress, 2nd Session, Public Law 472, Chapter 169]." National Archives and Records Administration, [On-line]. URL: http://www.nara.gov/exhall/featured-document/marshall/marshall.html (Accessed on 22 Jan. 2002.)

[13]William S. Cohen, *Strengthening Transatlantic Security: A U.S. Strategy For the 21st Century* (Washington, D.C.: Department of Defense, December 2000), v.

[14]The money was used to buy goods from the United States, which had to be shipped across the Atlantic on U.S. merchant vessels. But it worked. By 1953, the United States had pumped in $13 billion into Europe, and Europe was standing on its own feet again.

[15]For further reading, see John Gimbel, *The Origins of the Marshall Plan* (Stanford, Calif.: Stanford University Press, 1976); Imanuel Wexler, *The Marshall Plan Revisited: The European Recovery Program in Economic Perspective* (Westport, Conn.: Contributions in Economics and Economic History, 1983); and Michael J. Hogan, *The Marshall Plan: America, Britain, and the Reconstruction of Western Europe, 1947–1952* (Cambridge, Eng.; New York: Cambridge University Press, 1987).

[16]*Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century,* 7.

[17]In some areas, such as agricultural policy and trade, members of the EU pool their sovereign powers, which allows the EU to negotiate directly with the United States and other countries. In other areas, including international defense and security, members retain individual sovereignty.

[18]"The Goldwater-Nichols Department of Defense Reorganization Act of 1986, sponsored by Sen. Barry Goldwater [Rep.-Ariz.] and Rep. Bill Nichols [Dem.-Ala.], caused a major defense reorganization, the most significant since the National Security Act of 1947." See URL: http://www.ndu.edu/library/goldnich/goldnich.html (Accessed on 28 Feb. 2002.)

[19]David S. Alberts et al., *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd ed., rev. (Washington, D.C.: Command, Control, Communications, Computers, Intelligence Surveillance, Reconnaissance [$C^4$ISR] Cooperative Research Program [CCRP], August 1999).

[20]See Operation *Allied Force* [On-line]. URL: http://www.defenselink.mil/specials/kosovo/ (Accessed on 23 Jan. 2002.)

[21]Admiral William A. Owens, with Edward Offley, *Lifting the Fog of War* (New York: Farrar, Straus, and Giroux, 2000), 190-191.

[22]Myron Hura, et al., *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, Calif.: RAND Corp., 2000), 177.

[23]Interview by JoAnn Sperber, "Q&A: Interoperability Enforcer, Lt. Gen. Joseph K. Kellogg, Jr.," *Military Information Technology* **5**, 5 (2001), 19, [On-line]. URL: http://www.mit-kmi.com/archives/5_5_mit/5_5_index.cfm (Accessed on 12 Feb. 2002.)

[24]Dept. of Defense Directive no. 5000.1, 23 Oct. 2000, 2-3.

[25]Ibid.

[26]This observation is based on the author's experience in a tour at the Pentagon, where he found that the dedicated people who write policy almost always are well intended and are reasonable at practicing compromise.

[27]Personal communication to the author from Mark Mills, Captain, USN, within the Theodore Roosevelt Battlegroup, which, in the aftermath of the bombing of the world Trade Center towers and the Pentagon on 11 Sept. 2001, was conducting operations in the war against terrorism in Afghanistan in 2001–02 as this report was being written.

[28]John L. Less, *The Souring of the Defense Industry: U.S.-European Competition*, [On-line]. URL: http://www.sais-jhu.edu/studorgs/foreignobserver//1197/defense.html (Accessed on 13 Dec. 2001.)

[29]See Jacques S. Gansler, *Military and Industrial Cooperation in a Transformed, NATO-wide Competition*, [On-line]. URL: http://www.csdr.org/98Book/gansler98.htm (Accessed on 13 Dec. 2001.)

[30]Less, 1.

[31]Gansler, 2.

[32]An industry that is indigenous to a country or particular organization and not dependent on other sources for products or services is said to be "organic."

[33]CSIS, *Computer Exports and National Security: New Tools for a New Century* (Washington, D.C.: CSIS Press, A Panel Report of the CSIS Commission on Technology Security in the Twenty-First Century, June 2001), 7, [On-line]. URL: http://www.csis.org/pubs/; citing NSF, *Science and Engineering Indicators 2000* (Washington, D.C.: NSF, 2000).

[34]All figures here and throughout the study are given in U.S. dollars.

[35]Janne E. Nolan, "Cooperative Security in the United States" in *America's Strategic Choices*, edited by Michael Brown. (London, Eng.; Cambridge, Mass.: The MIT Press, rev. ed., 2000), 214.

[36]Briefing by Major General Rodney P. Kelly, *Deputy Chief of Staff, Plans and Programs*, distributed to Senior Service School Air Force Fellows 2001–2002 on 6 Aug. 2001, at Analytic Services, Inc. (ANSER), "a public-service institute, an independent, not-for-profit corporation chartered in California with the assistance of the RAND Corporation in 1958." See URL: http://www.answer.org/ (Accessed on 15 Jan. 2002.)

[37]Briefing by Bgen Faykes, *AF Budget Update*, distributed to Senior Service School Air Force Fellows 2001–2002 on 2 Aug. 2001.

[38]For example, briefing by Major General Rodney P. Kelly, *Deputy Chief of Staff, Plans and Programs*, distributed to Senior Service School Air Force Fellows 2001–2002 on 6 Aug. 2001.

[39]The following are recommended reading on the "Four Percent Solution": Frank J. Gaffney Jr., "The 'Four Percent Solution' for Military Readiness," *San Diego Union Tribune*, 13 Aug. 2000; Hunter Keeter, "Marine Commandant Calls for Defense Spending Increase," *Defense Daily*, 16 Aug. 2000, 6; Tom Stuckey (Associated Press), "Fleet Strength at Risk, Retiring Admiral Says," *Washington Times*, 23 July 2000, C-13; and Gordon R. Sullivan, editorial, "Increased Global Engagement Makes Greater Investment in Military Vital," *Tacoma News Tribune*, 18 Aug. 1998.

[40]Arthur Money, *Information Superiority: Making the Joint Vision Happen* (Washington, D.C.: U.S. Dept. of Defense, U.S. Gov't Printing Office, [2000]).

[41]Information superiority may be said to exist when one competitor can establish a relative information advantage over another, usually an adversary.

[42]Office of the Under Secretary of Defense for Acquisition and Technology, Final Report of the Defense Science Board Task Force on Globalization and Security (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, December 1999), [On-line]. URL: http://www.acq.osd.mil/dsb/globalization.pdf (Accessed on 27 Nov. 2001.)

[43]*Naval Research Advisory Committee Report*: *Science and Technology* (June 2000), 15, [On-line]. URL: http://nrac.onr.navy.mil/ (Accessed on 15 Jan. 2002.)

[44]Ibid., 37.

[45]Gordon R. Sullivan, editorial, "Increased Global Engagement Makes Greater Investment in Military Vital," *Tacoma News Tribune*, 18 Aug. 1998.

[46]Maintaining Military Advantage Through Science and Technology Investment (1995), [On-line]. URL: http://clinton4.nara.gov/WH/EOP/OSTP/nssts/html/chapt2.html (Accessed on 5 Feb. 2002.) The Science and Technology Program is heir to and expands the Advanced Research Projects Agency (ARPA), which, in the late 1960s, built ARPAnet, forerunner of the Internet.

[47]Ibid.

# Chapter Three

# Dual-Use Technology and Diffusion of Technology

> *This diffusion of explicitly military technology goes together with the problem of so-called "dual-use" technologies. If you can make semiconductors, you can put your chips in PCs, or in cruise missiles….*[48]
>
> Cosma R. Shalizi

Traditionally, national security concerns have motivated policies of the United States and its allies that support the development and implementation of advanced technologies. Defense programs dominated U.S. R&D during World War II and, as emphasized in the Marshall Plan, in its immediate aftermath. The payoffs were impressive, necessary, and appropriate to recovery. But over the next half-century, defense needs changed, and the ability of international defense organizations to fund all their needs also changed. At the opening of the twenty-first century, commercial competition, technological explosion, and diffusion have become the norm.

## 3.1 Dual-Use Technologies: Source of Answer or *Angst*?

Military leaders of today and tomorrow will need to gain considerable appreciation of dual-use technology in order to capitalize on its potential and avoid its pitfalls. The battlescape of international security has changed irreversibly, and the age of dead reckoning for success with military technology has past. Allies on defense battlefields may be adversaries on economic battlefields. Cyberspace has no borders: "in a single

second, a single strand of fiber-optic cable can transmit the data contained in 11,000 encyclopedia volumes."[49] For military equipment, commercial dual-use technology is the necessary "selection *du jour*":

> Dual-use technologies are technologies and goods that were developed for commercial use but which can be used either as military components or for the development or production of military systems.

Using this definition, this chapter examines how the DOD has embraced dual-use technologies, such as the Internet, as have adversaries and pirates in the globalized world.

Several industrialized nations, including the United States and many of its NATO allies, reserve the right to promote the proliferation of technology and, whether intentionally or unintentionally, may support the development or production, or both, of military systems abroad.[50] Globalization affects the DOD not only by altering the supporting industrial base but also by reshaping the military-technology environment.[51] The federal government now provides only 2 percent of the money that goes toward R&D, whereas in the 1950s it provided around 44 percent (see section **2.4**).

Globalization has forced the security elements of NATO to rely on dual-use technologies developed and initially produced in the commercial sector. To achieve information superiority, implement the Global Information Grid,[52] and, ultimately, conduct war successfully in a network-centric manner, the rising military leader will need to understand and employ dual-use technologies.

The formal Dual-Use Science and Technology Program that links the Services' researchers and developers to the commercial sector was established only in 1997. For the United States and its NATO allies to retain supremacy on the battlefields of tomorrow, their military leaders will need to follow the same objectives as the Program:

partnering with industry and jointly funding development of dual-use technologies. They will need to acknowledge that for industry to continue to bring revolutionary warfighting tools to the security establishments it will have to be competitive in the marketplace. According to Delores M. Etter, deputy under secretary of defense for science and technology, "the joint military and industry mission is to be sure that [the United States is] developing affordable and superior technology for the warfighter."[53] As stated in all joint vision documents, the manner in which the United States and its allies will fight in the future will depend on the ability to field superior technology. And according to John J. Garstka, a relative information advantage across the spectrum of conflict may be the most important factor for achieving information superiority.[54]

If the Dual-Use Program is intended to bring revolutionary systems into the military, then the Commercial Operations and Support Savings Initiative (COSSI) is the companion program that the U.S. military leader will need not only to know about but also to be fluent in its application. COSSI employs commercial technology to reduce the costs of operation and support (O&S) for military systems.[55] Like the Dual-Use Program, COSSI adapts off-the-shelf technology to improve warfighting tools, but, unlike the Dual-Use Program, COSSI supports military systems that have already been fielded—hence, the reduction in costs, particularly for legacy systems. According to Richard Mirsky, head of COSSI at the DOD's defense research and engineering office, "The initiative leverages private sector research and development and promotes civil military integration and supports acquisition reform."[56]

COSSI comprises a two-stage process. First, the DOD funds the nonrecurring engineering, testing, and qualification necessary to adapt a commercial item for military

use. Second, contractors are selected to develop, manufacture, and deliver prototypes to military customers for installation into fielded DOD systems. In the age of reduced defense dollars—the military leader of today and tomorrow will need to understand that only $10.8 million was requested for FY 2002—extending the life of military systems is critical just to maintain the capability that the DOD already possesses.[57] Extending the service life of military systems increases the costs of ownership (for example, O&S, including maintenance). Technology made available through COSSI increases component reliability and operating efficiencies by reducing costs for spare parts and maintenance. The gains in actual costs for the United States and its allies might be exponential if extending the lifecycles of existing military systems, such as aircraft and satellites, were to become standard practice.

### 3.2 Military Dual-Use Programs: Fertile or Feeble?

Imagine that all stakeholders are delighted with dual-use technologies and with the way in which the United States and its allies employ them to further international security. Imagine that the militaries get "revolutionary" equipment that gives them both information and technical advantages through dual-use. Imagine that, through COSSI, the militaries are infused with low-cost, fast-paced high technologies to improve systems already fielded. And imagine that, at the same time, the industrial base is alive and the commercial sector is both viable and delighted.

If a technology comes to be listed as dual-use in the military sense—"technologies and goods…developed for commercial use [that] can be used either as military components or for the development or production of military systems" (see section **3.1**)—then the technology will come under the processing rules of the Department of

State (DOS). The DOS's processing rules are, from the viewpoint of commercial industry, far too slow and have often been criticized for protecting or even prohibiting commercial sale of technologies already available globally. "No commercial firm doing international business wants [its technology] to [be under auspices of the DOS's licensing process]," according to Jack Nunn, who until 2001 for fifteen years headed the staff of the Dual-Use Science and Technology Program for independent assessment.[58]

Few commercial companies want to provide an enemy with a technology that could offer or increase an enemy's information advantage but, more important than blanket control—and more enforceable—is the need to focus on which technologies to control. Many potential military applications of commercial technologies can neither be understood by the military generally or by civilians nor policed by them. Complete control of every conceivable commercial product that might be used in a military manner appears impossible. The terrorists of September 11 used ordinary technologies: commercial telephones, on-line travel agencies, and the Internet.

Not all commercial companies want to do business with defense establishments around the world. Several have been "second sourced"—that is, an anticipated contract is given instead to a competitor that therefore did not need to pay for R&D or an engineering section. According to Jack Nunn, the U.S. commercial sector has complained of both excessive delays in payment and excessive oversight.[59]

In considering whether to participate in the Dual-Use Program, the rising U.S. military leadership will need to emphasize the benefits to industry, and industry, for its part, will need to be aware that it can indeed benefit—from cost-sharing among itself, the Office of Secretary of Defense, and the Services. For instance, a minimum requirement of

the current Dual-Use Program is that the DOD fund 50 percent of the cost. Through this Program a firm can develop and foster long-term partnerships with other firms and with defense labs and universities. Cost sharing can improve the potential for the transition of a technology into defense systems, which can then lead to increased markets globally. The rising military leader will need to foster such a win-win philosophy to the benefit of both the military and commercial industry.[60]

U.S. military leaders will have a role to play also in encouraging continued support not only for what the Dual-Use Program does but also for the Program itself. As **Table 3-1** shows, fiscal support for the program has slipped from a high of $68 million in FY 1998 to a steady state of

**Table 3-1. Funding for the Dual-Use Science and Technology Program**

| **Fiscal Year** | **Support** (millions) |
|---|---|
| 1997 | $65 |
| 1998 | 68 |
| 1999 | 30 |
| 2000 | 30 |
| 2001 | 30 |

Source: URL: http://www.dtic.mil/dust/faq.htm

only $30 million since 1999. Program dollars are revisited every year and are subject to congressional appropriation. The military leader's role in addition to employing the Program will be to praise it to congressional liaisons and constituents, wherever and whenever possible.

The DOD has come a long way in acquisition reform and in employment of dual-use strategies to capitalize on synergies between global commercial sectors and their companion defense establishments. Since the Clinton administration announced the

"21st-Century Defense Technology Strategy" (on 22 Feb. 1998), which called for building pillars of focus in R&D on dual-use technologies and emphasized reaching out globally for international cooperation, there has been significant progress.[61] Critical technologies are being advanced in information technology, manufacturing, materials, and advanced simulation.[62]

In a globalized world, economic and technological imperatives for increased reliance on the commercial sector by the DOD have required rethinking of how and where warfare will be conducted. The diffusion of technologies not even regarded as candidates for the Dual-Use Program or COSSI has been remarkable—and troubling. Such technologies have been neither monitored nor licensed by either the DOS or the Department of Commerce. After only a few years following reengineering, nearly all DOD business operations—and many critical military functions (e.g., logistics)—will be conducted over the Internet. For the United States and its allies, as also for their adversaries, the explosion of the Internet within the U.S. Transportation Command (USTRANSCOM) has been a harbinger of expanded use of the Internet to conduct military business.[63] The Internet has become a necessary tool for conducting warfare in the NATO scenario as well as a model of a dual-use technology that is nearly impossible to control.

### 3.3 The Internet and Its Diffusion Friends: Models for Limiting the Effectiveness of the DOD's Dual-Use Program

Like the United States, many countries have determined that in a knowledge-based economy it is essential to upgrade and privatize communications infrastructures and to make computers and access to the Internet widely available and affordable. Simply put, to remain competitive in this environment, access to and use of the Internet are

mandatory. Yet precisely that which allows collaboration among allies in peace also (like Janus) opens an opposing door for nefarious purposes. Today's Internet is not the ARPAnet of old.[64] Whereas ARPAnet and the early Internet were accessible mainly by government (primarily defense-related) and university researchers, today's Internet is accessible by anyone with a computer and a telephone connection, and such wide access is here to stay. The ten countries with the largest number of Internet hosts are (in descending order) the United States, Japan, Canada, Germany, the U.K., Italy, the Netherlands, Taiwan, Australia, and France.[65] Those with the greatest number of Internet hosts are (in descending order): China, Brazil, Iceland, Romania, Poland, Argentina, Taiwan, Hong Kong, Canada, and Portugal.[66] Canada has built the world's fastest, all-optical research network and connected all its schools to the Internet.[67]

The explosion of information technologies such as the Internet have serious implications for military and national security. The implications for international security intelligence and command and control are as old as Sun-Tzu.[68] But in 1998, during a U.S. military exercise, the computers and linkages that allowed the United States to communicate large amounts of information to allies in war were found to have another aspect:

> it only requires a modest capability that is easily available to seriously disrupt vital services like electric power distribution and telecommun-ications systems. A small handful of capable computer specialists—a capability well within the reach of even moderately developed countries—using off the shelf, existing tools and techniques can wage war on the largest nations in the world.[69]

The diffusion of technologies similar to computers and the Internet has become common. Some advocates of technological warfare talk of when war by bayonet will be replaced by war with computer viruses, logic bombs, and data manipulation. NATO's

allies and adversaries see the adoption of new technology as essential to their own economic growth and not as belonging exclusively to friendly English-speaking nations. Recent studies of technology diffusion have shown that the capacity to purchase and the ability to learn new technologies are more important than geographic boundaries.[70] Studies of the integration of computers into society have found that the source and type of trade with other countries are important determinants of technology diffusion, whereas the English-speaking share of the population has no significant effect.[71]

Diffusion and the use of computers and the Internet, which lie beyond the auspices of international dual-use programs (and export control laws), pose serious questions for today's military leaders and political leadership. On the Internet, what constitutes sovereignty? What are the limits of the right to self-defense when the United States can be attacked from a computer in one country over a telephone line that passes through two others? Should the use of cyberspace for military purposes be limited because the same cyberspace has become the backbone of the global economy? What kind of arrangements, Procedures, or treaties are needed that would simultaneously protect national security, promote electronic commerce (e-commerce), and communications, and preserve personal privacy? As is true of outer space, the management of cyberspace will require new regimes and approaches.[72]

Globalization has forever changed the military and political landscape. Increased use of the commercial sector to modernize existing military systems or to provide new ones has become standard. Increased reliance on the commercial sector by the United States and its NATO allies appears irreversible without the loss of certain significant gains, in particular in information-related technologies. Transatlantic partnerships, which could

yield returns in interoperability and maintainability, are ripe to strengthen the underpinnings of the defense industrial base and promote greater NATO cohesion.[73]

The establishment of a clearly articulated dual-use strategy that will be followed will be critical to success on the battlefields of the twenty-first century, whether those contested fields are on the ground, in the air, or in cyberspace. Shrinking dollars, mandatory extension of military systems, urgent interoperability concerns, and international competitive practices all drive the need for such a strategy, but international dual-use programs are accompanied by export controls and administration, which are the subject of **Chapter Four**.

Notes

[48]Cosma R. Shalizi, in a review of William W. Keller, *Arm in Arm: The Political Economy of the Global Arms Trade* (New York: Basic Books, 1995), in The Bactra Review (15 Feb. 1996), 1, [On-line]. URL: http://www.santafe.edu/~shalizi/reviews/arm-in-arm/ (Accessed on 20 Feb. 2002.)

[49]Linda D. Kozaryn, "Fast-Paced, High-Tech Advances Provide Winning Edge" *American Forces Press Service,* 14 Nov. 2000, [On-line]. URL: http://www.defenselink.mil/news/Nov2000/n11142000_200011141.html (Accessed on 16 Jan. 2002.)

[50]Janne E. Nolan, "Cooperative Security in the United States," in *America's Strategic Choices*, edited by Michael Brown (London, Eng.; Cambridge, Mass.: The MIT Press, rev. ed., 2000), 208.

[51]Final Report of the Defense Science Board Task Force on Globalization and Security (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, December 1999), [On-line]. URL: http://www.acq.osd.mil/dsb/globalization.pdf (Accessed on 27 Nov. 2001.)

[52]The Global Information Grid is the DOD's vision for implementing policy, process, and capabilities to ensure sensor-to-shooter integration.

[53]Jude E. Franklin, vice president and chief technology officer, Litton PRC, in an address to a conference on "Commercial Technology for the Warfighter" held by the DOD, McLean, Va., 8 Nov. 2000.

[54]According to Garstka, "Relative Information Advantage is achieved when one competitor outperforms its competitors in the information domain and performance in the information domain is relative to what information one needs." See John J. Garstka, "Information Superiority for the Warfighter," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-1, October 2001), 4 [On-line]. URL: http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=557 *Joint Vision 2010* (1996) defines information superiority as "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." See URL: http://www.dtic.mil/jv2010/jvpub.htm (Accessed on 16 Jan. 2002.)

[55]For the Commercial Operations and Support Savings Initiative (COSSI), see URL: http://www.acq.osd.mil/es/dut/cossi/FY02/Index.htm (Accessed on 31 Dec. 2001.)

[56]See URL: http://www.acq.osd.mil/es/dut/cossi

[57]For example, the infamous "fighter bathtub," which the OSD and the USAF have been trying to overcome until the Joint Strike Fighter and F-22 will be fielded.

[58]Personal communication to the author by Jack Nunn (31 Dec. 2001).

[59]Ibid.

[60]For a "Dual-Use Fact Sheet," see URL: http://www.dtic.mil/dust/faq.htm (Accessed on 4 Dec. 2001.)

[61]The three pillars are: reform the current Department of Defense (DOD) acquisition process, now biased against the use of commercial processes and products within defense systems; focus more R&D within DOD on dual-use products and processes, emphasizing the need to achieve advances in; high-tech defense systems that are affordable; and reach out globally to our allies, to benefit from international cooperation on a technology-by-technology basis. See URL: http://www.ibiblio.org/darlene/tech/report7.html (Accessed on 4 March 2002.)

[62]Defense Technology: The Payoffs for Economic and Military Security, [On-line]. URL: http://www.ibiblio.org/darlene/tech/report7.html (Accessed on 3 Dec. 2001.)

[63]Tasked with global transportation responsibilities in peace and war, USTRANSCOM uses the World Wide Web extensively to track passengers and cargo moving through commercial and military pipelines.

[64]ARPAnet, the foundation of the Internet, was the DOD's Advanced Research Projects network, built in 1968. See Martin C. Libicki, *Information Technology Standards: Quest for the Common Byte* (Boston: Butterworth–Heinemann, Digital Press, 1995), 251, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/libicki/libicki_quest/libicki_quest.html (Accessed on 29 Jan. 2002.)

[65]Internet Sizer, [On-line]. URL: http://www.netsizer.com/ (Accessed on 30 Nov. 2001.) See this site also for quantification of the enormous growth in the number of Internet hosts between from 1999 to 2001worldwide.

[66]Ibid.

[67]U.S. Department of Commerce Technology Administration, International Science and Technology: Policies, Programs, and Investments (December 2000), 3, [On-line]. URL: http://www.ta.doc.gov/Reports/itsw/SciTech2000.pdf (Accessed on 16 Jan. 2002.)

[68]Sun Tzu, *The Art of War: The Oldest Military Treatise in the World*, edited by Lionel Giles (Harrisburg, Penna.: Military Service Pub. Co., 1944), 51.

[69]Remarks by John Hamre at "Confronting the Security Challenges of the New NATO," the 15th NATO Workshop on political-military decisionmaking, Vienna, Austria,: 22 June 1998. See news briefing, Office of the Assistant Secretary of State, Public Affairs, URL: http://www.defenselink.mil/news/Jul1998/t07081998_t0622nat.html (Accessed on 3 Dec. 2001.)

[70]Francesco Caselli and Wilbur J. Coleman II, "Cross-Country Technology Diffusion: The Case of Computers," *National Bureau of Economic Research Digest* (July 2001), 1.

[71]Ibid.

[72]See Rachel Bronson and Daniel Goure, "Diplomatic Consequences of the Coming RMA: When the U.S. Is Unrivaled Militarily, What Happens to Our Alliances?" *Foreign Service Journal* (September 1998), ¶95, 2-4.

[73]Office of the Under Secretary of Defense for Acquisition and Technology, Final Report of the Defense Science Board Task Force on Globalization and Security (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, December 1999), [On-line]. URL: http://www.acq.osd.mil/dsb/globalization.pdf (Accessed on 27 Nov. 2001.)

# Chapter Four

# Export Control and International Positions

*Existing international and national controls over the export of nuclear materials and technologies…have demonstrate their low level of effectiveness.*[74]

General (Ret.) Remir F. Stepanov,
USSR, Head of Department,
International Fund for Social and
Economic Reform, Former Director
of Export Control (1992)

## 4.1 Export Control, International Security, and Interoperability

Because dual-use technologies fall under federal oversight, the control mechanism is export control law. Given the expanding international development of these technologies, the United States and other governments have come increasingly to use commercial business practices and technologies to reevaluate export control internationally. Current export controls were developed when manufacturing was local and only government-unique components were used.[75] As the United States and its allies reexamine their export control laws, for the sake of international security rising military leaders will need to watch the process carefully and contribute to the discussion. Were the defense establishment to be mute on changes in export control law, economic considerations might come to override security concerns.[76] The crossover of the DOD and commercial investment in technology occurred in the mid 1980s, leaving defense security concerns

and interoperability to play second fiddle. Technology transfer from commercial enterprise has become a competition among allied peers, but if security voices are not heard finance might lead the way.[77]

For NATO operations, the primary concern is the tie between export control and inter-operability. As allied nations build an indigenous capability, seek the lowest cost options for components (which often are external to NATO), and try to reduce the cycles for components, U.S. export laws drive them to look elsewhere for technology solutions, with potentially disastrous effects. According to a recent report by the Center for Strategic and International Studies (CSIS) on U.S. Military Export Control Reform, security procedures and export controls that were designed to protect U.S. security have increasingly become "the cause of security problems and may contribute to the worsening of interoperability problems within NATO seen during the air war in the Balkans."[78]

**4.2 Dual-Use Technologies and Export Control: A Necessary but not Ideal Marriage**

The security environment of the post-cold war world is different from that of the bipolar world in that it will increasingly require interdependence of the instruments of national power. To continue U.S. leadership in international security, the economic instrument will need to be used liberally and expertly. Export control laws may require modification from the cold war construct still current in 2002 to recognize transnational partnership in certain areas: entire end-items or their components; globalization of the Internet; diffusion of technology; increased reliance on commercial solutions for military capability; and a waning domestic defense capability (see **Chapters Two** and **Three**).

In many respects, civilian technologies have caught up with or surpassed military tech-nologies. The military may no longer have a preponderance of or preeminence in

technologies, yet to maintain information superiority—even, perhaps, at the expense of interoperability—the United States cannot afford to surrender primacy in information technologies. The interoperability of military systems is enhanced by the sale or export of dual-use technologies in three ways: (1) exports enhance U.S. security by ensuring that allies have the same or similar equipment; (2) exports defray the costs of development and maintain a viable manufacturing capability for future sales and, presumably, for greater stability; and (3) because exports support the economies of allies, they allow the United States to "profit" through allies' goodwill. But throughout the NATO alliance there are challenges to export control laws.

### 4.3 Recognition of Weaknesses in Export Control

The commercial sector does not like to have the technologies it develops and produces under federal oversight, but for a technology to be licensed it must be processed either by the Department of Commerce or the DOS (see section **3.1**). This system has been choking on the volume of applications for routine technology being exported to friendly countries. The Cox Commission called on the United States to build "higher fences" around a smaller set of critical components while attempting to control fewer goods.[79]

This volume of applications has led to a situation in which most of the U.S. military licenses granted each year have been approved or denied with little scrutiny or debate. The military leader has had and will continue to have a role in articulating the need to control sensitive or unique technologies and in helping to establish measured, disciplined, enforceable processes based on security and stability, not economics. Processes built on political compromise will not always have national or international security interests at

heart. Of approximately 55,000 applications for licenses or for agreements processed annually through the DOS, for example, less than 20 percent will be referred to other agencies for review and less than 1 percent will be referred to Congress.[80] The military leader of today and tomorrow will need to fight against bureaucratic export control solutions—increasingly common in the absence of unanimity on U.S. objectives.[81]

An important nuance of export control has been the "blanket prohibition" of technologies. Many governments place such prohibitions on technologies with commercial interests, for example, space-launch vehicles. These prohibitions might be acceptable, except that often lobbyists apply political pressure and are granted waivers to them. As a result, the technology soon diffuses to secondary and tertiary customers and the blanket becomes unenforceable. This situation represents the worst-case scenario: "unenforceable export controls with no ability to monitor either the destination or uses of transferred technologies."[82]

The globalization of "dual-use" technologies combined with ineffective export controls threaten transatlantic security. Determining whether a commercial product is a military application can be more an art than a science. Although commercial airliners may be used as military airliners, before September 11 few people would have imagined one military application for them could be missile technology. In information technology, the line between commercial and military applications is fuzzy at best. According to William Keller, if you can make semiconductors, you can make personal computers for organizing food recipes or chips for cruise missiles.[83]

A staunch export conservative may find it alarming that an adversary possesses the power of a 486 microprocessor and thereby "more computing power than United States

scientists had when they developed the first atomic bomb."[84] But military applications do not require a high MTOPS (millions of theoretical operations per second) computing power. The air superiority fighter for the twenty-first century, the F-22, for example, "was designed with a 958 MTOPS Cray supercomputer, roughly one-quarter the power now found in mass-produced Pentium chips."[85] Diffusion of explicitly military technology is an eventuality as the line between military and civilian dual-use blurs. Information technologies may be the most difficult to control owing to their lucrative and legitimate nature. Electronics, computers, telecommunications, and information security all are on the Wassenaar Arrangement (WA) Dual-Use Control Lists of sensitive dual-use items, yet the United States and several of its allies export these items simply because they are so lucrative.

### 4.4 Export Control Policy: Boiling Debate

Under the WA, participating states notify one another of denials of exports of sensitive dual-use items. They also inform all other participating nations that have approved a license for a transaction denied by another member within the last three years. To strengthen bilateral consultation before authorization of an export of a dual-use technology, the United States proposed adoption of a procedure for notification of denial that is similar to that used by other multilateral export control regimes. In the proposed procedure, before approving exports the participating states would consult with other participating states that deny the export of similar items to the same end-user. Adoption of "denial consultation" would be relatively painless for the participating states, given that "In the first two and half years of the [WA] there were only forty reported denials of Sensitive List and Very Sensitive List items."[86]

The Dual-Use Control Lists are extensive, and forty reported denials make for a relatively small number.[87] The position of the United States has been to increase strategic security by reducing the opportunity for a potentially nefarious end-user to "shop around" for dual-use technologies that could aid or abet a military application. The United States is not alone in reviewing export laws in light of the globalization of the marketplace and of emerging technologies. Its NATO allies also have seen the globalization of information technology as both an economic center of gravity and a catalyst for control of exports and, for these reasons, have begun to review their own laws. For example, the United Kingdom's Import, Export, and Customs Powers (Defence) Act, written in 1939, has been criticized at home and has begun to be revamped. In 1998, the U.K.'s Department of Trade and Industry published a White Paper on the modernization of strategic control powers to accommodate modern means of trading, such as transferring information over the Internet and brokering deals that involve the transfer of goods between two countries.[88]

The U.K. and the United States share some concerns. Both countries remain committed to transatlantic security and to providing greater transparency of export items, but neither wants its own industry to sacrifice a competitive advantage in the global marketplace. According to the 1998 White Paper, "any process involving publication of individual applications…would mean identifying companies and the nature of their planned or actual export business which would likely harm their competitive advantage."[89]

The U.K. has been concerned that foreign governments that have been buying technologies will look elsewhere for their next purchase, that is, to a country with less

transparent export laws. Before 1996, national and international export control systems were primarily the domain and responsibility of individual nations acting in their own best security and economic interests. Many countries, however, following the lead of the United States and Russia, recognized that to ensure international security "the emergence of transnational business and industrial partnerships requires a new model of government oversight,"[90] and toward that end in July of 1996 the United States and thirty-two other countries, including all members of NATO with the exception of Iceland, signed the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. To be admitted to the WA, a country must be a producer or an exporter, or both, of arms or sensitive industrial equipment.

Participating nations agree to report on certain categories of export approvals of licenses or transfers and denials of licenses to nonmembers. The objective of the WA is to encourage

> transparency, consultation, and, where appropriate, national policies of restraint foster greater responsibility and accountability in transfers of arms and dual-use goods and technologies.[91]

The urgency of establishing international export control oversight in the post-cold-war security environment would seem obvious, yet debate and then agreement on the WA by the thirty-three nations took three years. The U.S. ambassador to the WA, David T. Johnson, although "reasonably impressed" with progress thus far (as of early 2002), has pointed out that the United States can ill afford to be complacent about the Arrangement.[92] The items that fall under its auspices are legal and lucrative, and in an economically competitive global environment the challenge is to muster the political will and exercise the national discipline to control such technologies.

Key to the success of the WA, as has been true of other international trade and export agreements, will be communication within and among the United States and its allies. Bulgaria's effort to join NATO offers an example of communication on international trade that can lead to increasing security, but its effort to control exports of arms and dual-use technologies illustrates the problem: the siren of dollars woos a nation desirous of collective security and stability. Desirous of admission to NATO and the EU, Bulgaria, through the WA, has agreed to implement a "responsible" arms trade policy consistent with the EU's Code of Conduct on Arms Exports, which lists export criteria as a guide to decisions on whether to grant or refuse an application for an arms export license.[93] And therein lies the rub. Bulgaria hopes to improve its chances of gaining entry into NATO and the EU by demonstrating that it is a good world citizen, but "its domestic legislation has yet to incorporate international regulations to which the country has committed."[94] Bulgaria lags, in part because its regulatory enforcement remains weak while incentives to export are strong.

The importance of NATO, and its Treaty, as an enabling force for international security cannot be overestimated. Bulgaria and other former Warsaw Pact nations regard NATO as underpinning their national security, too. Thus, the United States has the opportunity to build on the structure of NATO and other international organizations to spread the message, and reality, of information technology interoperability consistent with transatlantic security.

The rising U.S. military leader will need to become familiar with DOD Directives, in particular DODD 2040 (2002) on International Transfers of Technology, Goods, and Services of 1985. In an effort to take responsibility for achieving security with the

economic instrument of national power, DODD 2040 states that defense-related technology ought to be treated as a valuable, limited resource, to be husbanded and invested in in pursuit of national security. It also recognizes the importance of international trade to a strong U.S. defense industrial base and therefore directs the DOD to apply controls in a way that will interfere only minimally with legitimate trade and scientific endeavor.[95] Debate in the U.S. Senate on the Export Administration Act of 2001 suggests the interests, security and economic, that need to be weighed.[96] A week before the attack on September 11, Senator Fred Thompson (Rep.-Tenn.) said that the Senate "[is] debating legislation that weakens our export control practices in order to enhance our commercial interests."[97]

### 4.5 The Internet and Export Control

Will the Internet promote a breakdown of all export control laws, and are the United States and its allies merely punishing firms that are trying to conduct business? Stakeholders in international security will only delude themselves by believing they can limit the export of technologies critical to security but already in the public domain and which may already be being used for organized crime, espionage, and terrorism. Further complicating the debate on export control of information technologies is one particular apparently ubiquitous information technology: the Internet.

The Internet has rendered debate on export controls of some dual-use technologies such as encryption meaningless. Encryption software has already gone into public domain, spread there in the 1990s, in Debora L. Spar's phrase, by "pirates and well-wishers" who distributed key algorithms by using the Internet:[98]

> the advent of the Internet seemed to shift power away from the state. Pushed by technology that was evolving much faster than policy, national governments abandoned their restrictions on high-powered encryption or, as in the U.S. case, weakened them substantially.[99]

Diffusion of technologies such as the Internet along with the exchange of other information technologies or of data riding on the Internet may seriously jeopardize national security.

### 4.6 Export Control and Russia

The need to balance the conflicting demands of national security and economic growth and development is not unique to the United States and its NATO allies. Russia also has been struggling with the Janus faces of this dilemma and with how best to achieve a balance. Russia's technologies need to be controlled for security purposes, yet, at the same time, Russia needs to unleash them to stimulate desperately needed economic growth.

The need for controls on export between the United States and Russia of dual-use technologies relevant to the development and deployment of weapons will diminish as relations between these nations improve and greater trust is established, overcoming the legacy from the cold war of mutual suspicion and fear of threat. The rising military leader will need to understand that continuing improvement in political and economic relations and the growth of mutual trust, like that between NATO and Japan, are possible.[100] The terrorist attack of September 11 and the apparently warm relations between President George W. Bush and Russia's President Putin seem to have improved relations also between NATO and Russia, as was evident later that month, when General Anatoly Kvashnin, Chief of the General Staff, told RIA-Novosti, the Russian Information Agency, that relations were moving from the theoretical plane toward practical

cooperation in international stability.[101] The Russian Federation is already a member of the WA and could prove a stabilizing force in export controls.

International debate on export controls and security will probably continue as the global environment of free trade, workforce migration, and international competition, mixed with emerging threats and enlarging alliances, continue to drive nations to reconsider both domestic and foreign interests.

## Notes

[74]Remir F. Stepanov, "Basic Trends in the Development of Mechanisms for Controlling the Export of Dual-Use Products," in *Dual-Use Technologies and Export Administration in the Post-Cold war Era;* documents from a joint program of the National Academy of Sciences and the Russian Academy of Sciences/Office of International Affairs, National Research Council (Washington, D.C.: National Academy Press, 1994), 139.

[75]CSIS, Executive Summary, *Technology and Security in the Twenty-First Century: U.S. Military Export Control Reform* (Washington, D.C.: CSIS Press, A Panel Report, May 2001), 6, [On-line]. URL: http://www.csis.org/export/execsum.htm (Accessed on 16 Jan. 2002.)

[76]The need for military leaders to contribute to the discussion on export control can be likened to the discussion that was almost not held on the sale of the frequency spectrum, in which economic considerations nearly outweighed security concerns about interoperability.

[77]Quoted by Cosma R. Shalizi, in a review of William W. Keller, *Arm in Arm: The Political Economy of the Global Arms Trade* (New York: Basic Books, 1995), in The Bactra Review (15 Feb. 1996), 1 [On-line]. URL: http://www.santafe.edu/~shalizi/reviews/arm-in-arm/ (Accessed on 20 Feb. 2002.)

[78]CSIS, Executive Summary, *Technology and Security in the Twenty-First Century: U.S. Military Export Control Reform* (Washington, D.C.: CSIS Press, A Panel Report, May 2001), 3 [On-line., URL: http://www.csis.org/export/execsum.htm (Accessed on 16 Jan. 2002.)

[79]Ibid., 7. See Christopher Cox (Rep.-Calif.): "In the 105th Congress, Rep. Cox served as chairman of the [bipartisan] Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China… created…June 18, 1998, [which] unanimously approved its report December 30, 1998, prompting major legislative and administrative action. The unclassified version of the report was issued in three volumes in May 1999." According to the Select Committee, the PRC has been stealing from the U.S. National Laboratories, as early as the 1970s and as recently as the mid-1990s. See URL: http://www.house.gov/coxreport/ (Accessed on 21 Feb. 2002.)

[80]Janne E. Nolan, "Cooperative Security in the United States," in *America's Strategic Choices*, edited by Michael Brown (London, Eng.; Cambridge, Mass.: The MIT Press, rev. ed., 2000), 211.

[81]Ibid.

[82]Ibid., 212.

[83]Cosma R. Shalizi, in a review of William W. Keller, *Arm in Arm: The Political Economy of the Global Arms Trade*.

[84]Philip Heerman, computer scientist, Sandia National Laboratories, quoted by Jeremy Hay, in "Fun and War Games," *Wired* (April 2001), [On-line]. URL: http://www.wired.com/wired/archive/9.04/mustread.html?pg=11 (Accessed on 21 Feb. 2002.)

[85]Seymour E. Goodman, Peter Wolcott, and Patrick Homer, *High-Performance Computing, National Security Applications, and Export Control Policy at the Close of the 20th Century (*Washington, D.C.: U.S. Dept. of Commerce, Bureau of Export Administration, 1998), 15.

[86]For the United States's "Position on Strengthening Wassenaar's Dual-Use Procedures," see URL: http://www.usun-vienna.usia.co.at/wassenaar/position04.html (Accessed on 9 Oct. 2001.)

[87]Participating states agree to control all items set forth in the list, which has two annexes, of sensitive and a limited number of very sensitive items. The list is reviewed regularly to reflect technological developments critical to indigenous military capabilities. For the computer list, see URL: www.wassenaar.org/list/Cat%204%20-%2099.pdf (Accessed on 4 March 2002.)

[88]For the White Paper, see the Department of Trade and Industry, Strategic Export Controls, Presented to Parliament by the President of the Board of Trade by Command of Its Majesty, July 1998, [On-line]. URL: http://www.dti.gov.uk/export.control/stratex/1sec.htm (Accessed on 9 Oct. 2001.)

[89]Ibid., Section 2, Accountability in Strategic Export Controls, 3, [On-line]. URL: http://www.dti.gov.uk/export.control/stratex/2sec.htm (Accessed on 9 Oct. 2001.)

[90]CSIS, Executive Summary, *Technology and Security in the Twenty-First Century: U.S. Military Export Control*, 9.

[91]See The Wassenaar Arrangement, Questions and Answers, [On-line]. URL: http://www.usun-vienna.usia.co.at/wassenaar/WAQ&A.htm (Accessed on 9 Oct. 2001.)

[92]David T. Johnson, Opening Statement of the 12 Feb. 1999 Meeting, Wassenaar Arrangement Assessment, [On-line]. URL: http://www.usun-vienna.usia.co.at/wassenaar/johnson01.htm (Accessed on 9 Oct. 2001.)

[93]The EU's Code of Conduct on Arms Exports seeks to create "high common standards" that are politically binding on members' arms export decisions and to increase transparency on arms exports among EU members.

[94]Annemarie van Berkel, "Bulgaria's Arms Trafficking: An Issue Yet to Be Resolved," *Weekly Defense Monitor* **3**, 46 (2 Dec. 1999), 1, [On-line]. URL: http://www.cdi.org/weekly/1999/issue46.html#2 (Accessed on 28 Feb. 2002.)

[95]DOD Directive no. 2040, 2, 17 Jan. 17, 1984; Administrative Reissuance Incorporating Change 1, July 5, 1985.

[96]U.S. Senate Committee on Banking, Housing, and Urban Affairs, Committee Documents Online—107th Congress, Summary: The Export Administration Act of 2001, 23 Jan. 2001, [On-line]. URL: http://banking.senate.gov/docs/eaa/summ01.htm (Accessed on 4 March 2002.)

[97]News release, Senator Fred Thompson (Rep.-Tenn.), Thompson Statement on Export Administration Act [S.149], *Congressional Record*, 4 Sept. 2001.

[98]Debora L. Spar, *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth from the Compass to the Internet* (New York, San Diego, London: Harcourt, 2001), 247.

[99]Ibid., 248.

[100]Office of International Affairs, National Research Council, *Dual-Use Technologies and Export Control in the Post-Cold War Era: Documents from a Joint Program of the National Academy of Sciences* (Washington, D.C.: National Academy Press, 1994).

[101]From Moscow RIA–Novosti, the Russian Information Agency, part of the state media holding company, and found in a daily press highlight for Air Force Fellows, 20 Nov. 2001 (in Russian).

## Chapter Five

# Conclusions and Suggestions

In the globalized world of the twenty-first century, the rising military leader will not be able to expect to conduct strategic operations in a vacuum of the military instrument of national power but, instead, will need to be able to contribute to the debate involving several instruments of national power: political, economic, and informational. An examination of transatlantic security and globalization through the lens of the economic instrument suggests that this huge aspect of the elephant remains to be explored.

Within the North Atlantic Treaty, military and commercial investment in technology, particularly dual-use technologies, and export control provide grounds for conclusions and suggestions that, especially for the rising NATO military leader, may prove useful and which, along with a developing understanding of international globalization may offer launch points for the discovery of other elements for later investigation.

Globalization has mandated that the military leader learn the languages of economics and high-technology and apply them in an effort to aid international stability. The focus of this study has been primarily on transatlantic security, but, given that NATO essentially underpins world security, lessons learned in and around the Atlantic theatre may be extrapolated to the global scene.

The invocation on September 12, 2001, by NATO of Article V of its Treaty, which enforces collective security and military response, demonstrated that this commitment remains important for global security. Beyond fulfilling it, military leaders of today and tomorrow will need to be able to contribute to stability also by articulating their role in implementing Article II, which calls for ensuring stability through economic means.

Warfare in the future will be conducted by coalitions, will rely on advanced technology, and will depend on interoperable systems and structures. Achieving interoperability will remain a worthwhile objective, but issues of national sovereignty and healthy economic competition may diminish the implementation of interoperability. In the era of cyberspace and cyberwar, diffusion of technologies may overcome even well-intended export controls of military materiel, complicating the pursuit of interoperability. For NATO to maintain its military superiority it will need to adapt to, fund, and implement a balance of defense and economic priorities that will themselves then be balanced against international cooperation.

The European Union is the most viable instrument for achieving a lasting economic balance in transatlantic security. As the United States's largest trading partner—accounting for more than $500 billion in two-way annual trade—the EU is a blockbuster and likely to grow even more important through the acceptance in most of Europe of a common currency. The United States and Europe have approximately $4.5 trillion invested in each other's economies, and rising military leaders on both sides of the Atlantic will need to leverage that investment for security purposes that support interoperability.

Although a two-way investment of $4.5 trillion may seem singularly impressive, it may, as shown in this study, suggest an altogether different picture of international defense spending and investment. As of early 2002, all members of NATO were suffering from declining defense budgets and declining competing economic interests. The opportunity for international cooperation exists, yet the watchword these days would seem to be competition. The United States has been spending nearly six times more than its next ally on national defense, and the NATO allies have shown no concerted effort to close that gap. Instead, their investment in defense has stayed largely flat over several years (see **Figure 2-3**). The rising U.S. military leader will need to temper an appetite for goldplating systems in requirements decisionmaking.

The shrinking international defense trade has led to a souring of relations between the EU and United States. In a global environment of decreasing defense spending, a decreasing defense industrial base, and a commensurate rise in the costs of military operations and maintenance, interoperable systems will be difficult to achieve. The opportunity for cooperation exists, but the globe remains plagued by nationalism. Because each and all of the NATO allies has its own indigenous manufacturing, assembly, and research capabilities in the defense and high-technology industries, controversy over how best to reach consensus on international trade will undoubtedly continue.

In addition, given that the type of warfare most probable in the future is coalition warfare, and given that interoperable systems aid coalition warfare, the rising military leader will need to articulate the requirements of global warfare. Should a shortfall exist

in the NATO alliance, the military leader will need to be able to state the requirements objectively, unbiased by national economic objectives.

Defense spending as a percentage of the GDP has slipped to its lowest point since the end of World War II, yet modernization of weapons systems appears paramount in order to achieve information superiority. Recognizing that, the rising military leader will need to push for increased defense spending as a percentage of the GDP. With that push comes the need to be able to delineate clearly any warfare shortfall as well as concrete plans to achieve fiscal responsibility.

Military leaders will need to be familiar with the DOD's Science and Technology Program as well as able to apply it to enhance security both at home and abroad. By providing technologies that aid evolutionary change, such a program may prove a valuable instrument for furthering warfare in a network-centric environment. It may prove important to the military leader also because, with the decrease in defense spending for R&D, the DOD's ability to influence high-technology advancement has been marginalized. The rising military leader will need to leverage this program in order to fill niches in technology where the commercial sector either is not the champion or is wanting. The United States's reliance on information superiority to enable dominance in operations and logistics itself relies on technological niches that will need to be filled through recourse to this program.

In an outgrowth of globalization, several nations have reserved their right to promote the proliferation of technology and to encourage their own commercial industries to export liberally. As a result, the defense and security stakeholders, both military and economic, will need to rely on dual-use technologies that may have originated in the

commercial sector. Such dependence, although troubling to the U.S. military officer, will most likely prove necessary, because whereas in the 1950s the federal government provided nearly 45 percent of the R&D dollars, it now (2001–02) provides only 2 percent. The military leader will therefore be dependent on dual-use technologies to achieve information superiority, to implement the Global Information Grid, and, ultimately, to conduct network-centric war.

Diffusion of technology that could be used for military purposes against members of the NATO alliance remains an increasing threat. Now nearly ubiquitous, computers and the Internet have been used for attacks on computer networks and for terrorism. The military leader will need to regard the Internet as a model of the military potential of technology diffusion and become educated about the means of diffusion available to pirates and criminals.

The rising military leader will need to be less naïve than at present about the military implications of the explosion of global technologies and will need to work to minimize NATO's vulnerability to attack. Globalization has rendered the Eurocentric mindset of the past less relevant now that geographic boundaries and English-speaking nations have become simply part of the global herd and certainly no longer solely dominant in technology transfer. Questions of sovereignty, right of defense, and the limits of cyberspace have ascended, and rigid defense structures have become passé.

Export control of military systems and dual-use technologies that may be used in military applications has become critical to maintaining international security, along with acceptance of the increasing obsolescence of current export practices and processes. As a recent in-depth study has suggested, current U.S. export control practices may even

contribute to interoperability problems in the NATO alliance.[102] Such problems arise, for example, when export control practices squeeze legitimate business exports or make processing so difficult that locating alternate sources of technologies becomes expeditious, which lead to an environment with disparate systems. By being neither obstructionist nor mute on export control of technologies that might aid inter-operability, the rising military leader will ultimately aid international stability.

Exports clearly can enhance U.S. security by ensuring that allies have the same or similar equipment, defraying costs of development, and maintaining a viable manufacturing capability for future sales. By articulating the need for control of sensitive or unique technologies and by helping to establish measured, disciplined, enforceable processes, based on security and stability, and not simply economics, the rising military leader will have an impact on and will be able to assist in—and would be well advised to do so—building unanimity concerning NATO's defense objectives and the associated export controls.

For reasons of transatlantic security, continued participation by NATO members in the Wassenaar Arrangement would seem mandatory as well as continued encouragement of full participation in the WA by the Russian Federation, particularly in regard to exports with a high probability of reaching unintended third parties. Full disclosure of previously denied exports would strengthen transatlantic security, and, to date, although such denials have been few, any denial of material with military applications will enhance security. Full participation in Wassenaar would help to reduce the number of potential adversaries that would "shop around" in order to exploit technology for nefarious purposes.

Finally, a premise of this study is that globalization appears irreversible. To remain relevant on the stage of international security, the rising military leader in NATO and the United States, rather than having a solely military perspective, will need to have a broad perspective on international stability. Such a leader will need to be part diplomat and part economist while also retaining a military outlook.

## Notes

[102]CSIS, *Technology and Security in the Twenty-First Century: U.S. Military Export Control Reform* (Washington, D.C.: CSIS Press, A Panel Report, May 2001), [On-line]. URL: http://www.csis.org/export/ (Accessed on 16 Jan. 2002.)

## *Acronyms*

| AOR | AREA OF RESPONSIBILITY |
|---|---|
| $C^4ISR$ | Command, Control, Communications, Computers, Intelligence Surveillance, Reconnaissance CCRP |
| COCOM | Coordinating Committee for Multilateral Export Controls |
| COSSI | Commercial Operations and Support Savings Initiative |
| CCRP | Cooperative Research Program |
| CSIS | Center for Strategic and International Studies |
| DOD | U.S. Department of Defense |
| DOS | U.S. Department of State |
| EU | European Union |
| FY | fiscal year |
| INSS | Institute for National Strategic Studies |
| MTOPS | millions of theoretical operations per second |
| NATO | North Atlantic Treaty Organization |
| O&S | Operations and Support |
| OSD | Office of the Secretary of Defense |
| TOA | Total Obligation Authority |
| U.K. | United Kingdom |
| USAF | United States Air Force |
| USSR | Union of Soviet Socialist Republics |
| USTRANSCOM | U.S. Transportation Command |

| | |
|---|---|
| WA | Wassenaar Arrangement |
| WWW | World Wide Web |